REMARKS

In response to the Office Action mailed on January 30, 2007, Applicant(s) respectfully request(s) reconsideration.

Claim(s) 1-34 are now pending in this Application.

In this Amendment, claim(s) 1, 10, 20, 29, 30 and 32-34 have been amended and claims 5 and 21 have been cancelled.

Claims 1, 10, 20, 29 and 32-34 are independent claims and the remaining claims are dependent claims.

Applicant(s) believe that the claim(s) as presented are in condition for allowance. A notice to this affect is respectfully requested.

Rejection under 35 U.S.C. §101:

Claims 32 and 33 have been rejected as being nonstatutory. Accordingly, Claims 32 and 33 have been herein amended to recite an encoded set of processor based instructions defined as program code on a computer readable storage medium, to bring the subject matter of the claims within 35 U.S.C. §101. It is therefore respectfully requested that the rejection under 35 U.S.C. §101 be withdrawn.

Rejection under 35 U.S.C. §102(e) based on Kato, et al., U.S. Publication No. 2002/0040431:

Claim(s) 1-34 were rejected under 35 U.S.C. §102(e) as being anticipated by Kato, et al., U.S. Publication No. 2002/0040431 (Kato '431). Applicant(s) respectfully disagree with these contentions and assert that the present claimed invention is not anticipated by any disclosure in the Kato '431 references.

Specifically, the Office Action rejects claim 1 based on the suggestion that Kato teaches the claimed transmitting of the signature block. In the Kato '431 disclosure, however, Kato teaches selective assignment and signature generation via a graphical user interface [0017]. The cited [0030] paragraph

teaches assignment and manipulation of signed elements, albeit via a remote processing function 33. Kato employs a signature template for designating a placeholder for a subsequent signature written by the sending node. In contrast, the claimed approach employs a signature block operable by a nonsigning client (i.e. not controlling encryption capability) on only the unsigned payload, not for manipulating the signatures of the signed element. In this manner, the claimed invention teaches a sending client node that does not compute the signature and is not encumbered by signature infrastructure.

In further detail, in the subject application, the client processes a message to store, in the information object portion, payload data in a nondestructive manner, the nondestructive manner operable to preserve the covered data portion and corresponding signature without regenerating the signature, as recited in claim 1. Thus, the claimed invention differs from the cited Kato reference because the generated signature from the server is not reconstructed or overwritten once received form the signature generating server. In contrast, Kato teaches a system in which the sending node performs encryption [91,108, 109] and Fig. 5. Clarifying further, while Kato appears to maintain some sort of remote link to the signature processing function 33 [0092-0094], the invocation and control of the encryption remains with the sending node as the sending node overwrites a placeholder template with a signature from the signature processing function during the course of assembling the message [0123].

Accordingly, while it is believed that claim 1 is distinguishable from Kato '431 based on the above observations, Applicant has herein amended claim 1 with the subject matter of claim 5, to clarify that storing in the information object portion further comprises storing the payload data at a client, the client being unencumbered by signature generation operability, to further clarify and distinguish applicant's claimed invention.

While the Office Action suggests that Kato teaches claim 5 at paragraphs [0080] and [0088], Kato teaches inserting a generated signature to overwrite a template signature. Since the inserted signature is generated on demand in

response to a GUI selection [0074], Kato does not show, teach, or disclose the client unencumbered by signature generation operability. Since Kato retains control over and invokes the signature processing function 33, Kato cannot be said to be unencumbered by signature generation capability, a necessary function of an encryption infrastructure, the overhead of which the present invention seeks to avoid.

The Kato '431 approach interactively prompts, computes, and adds a signature to an existing message, as discussed at paragraphs [0115,0116]. The sending node 10 identifies the elements to receive the signature [0117], selects keying material for generating the signature [0119], and invokes the processing for generating the signature from the keying material (i.e.) and the data to be signed [0123]. In contrast, the claimed invention does not perform nor require selection of keying material or invocation of the encryption operation, as shown at page 7, lines 23-28. Thus, while Kato suggests that the key processing may occur remotely ([0092-0094]), such encryption processing g is nonetheless under the direct control and invocation by the sending node 10. In contrast, the claimed sending client requires no direct or immediate control to the encryption processing.

In further contrast, as stated in [0088], since the Kato GUI selection overwrites the signature element of the XML message, Kato does not show, teach or disclose storing in a nondestructive manner. It is therefore respectfully submitted that amended claim 1 is allowable over the cited Art of record, and it is respectfully requested that the rejection under 35 U.S.C. §102(e) be withdrawn. Further, claim 10, rejected on similar reasoning, has been likewise amended with the subject matter of claim 13 and is therefore believed allowable.

The Office Action further rejects claim 20 based on Kato '431. Claim 20 is distinguishable from Kato because Kato does not show, teach, or disclose a signature value portion in the signature block. Kato requires a signed template operable as a placeholder for a pending signature. The cited Kato '431 publication does not show, teach, or disclose a signature template. In contrast,

the claimed invention employs a signature value field, employed by the signature server for storing the signature value. The signature value field is distinguishing because the signature value field is not manipulated or rewritten by the client once the signature value is stored at the server.

Therefore, the Kato approach provides a mechanism for aggregating signatures on successive parts of the message, and employs a template for temporarily buffering an XML field for the eminent signature, but in either case performs the same signature generation directly from the sending node. Claim 20 has been herein amended with the subject matter of claim 21, to clarify that the signature block further includes a signature value portion, the metalanguage processor further operable to store, in the signature value portion, authentication indicators according to the predetermined protocol, wherein storing further comprises storing the signature in the signature value portion.

Claims 32 and 34, likewise rejected, have been amended with the subject matter of both claims 5 and 21, as discussed above, to further clarify and distinguish the invention of these claims over the Kato reference.

Claim 29, also rejected on the Kato '431 reference, has been further amended with subject matter of claim 30, to clarify that the signature value portion and corresponding signature value persist as a signature block according to the predetermined protocol including the payload data portion, to further clarify the unmodified, unwritten nature of the signature in distinction from Kato. In Kato '431, A signature target adding method F12sig generates and adds the signature to preexisting message [0109]. The generated signature is replaced in the message, as discussed at [0110]. In contrast, the claimed invention receives signatures and augments non-signed fields (i.e. payload) and avoids performing encrypting or writing signature blocks, as disclosed at page 6, line 26-page 7 line 3. In amended claim 21, the nonsigning client (i.e. sender of the message) only writes payload data into the unsigned block, and does not manipulate preexisting signature values in signed blocks, as disclosed at page 7, lines 18-25. Claim 29 has been further amended with subject matter from claims 21 and 5, as

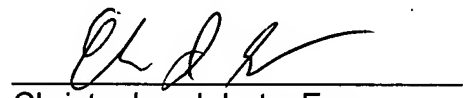
discussed above, in further distinction of Kato. Claim 33, rejected on similar grounds, has been likewise amended.

As the remaining claims depend, either directly or indirectly, from claims 1, 10, 20 and 29, it is respectfully submitted that all claims in the case are now in condition for allowance.

Applicant(s) hereby petition(s) for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3735.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-9660, in Westborough, Massachusetts.

Respectfully submitted,



Christopher J. Lutz, Esq.
Attorney for Applicant(s)
Registration No.: 44,883
Chapin Intellectual Property Law, LLC
Westborough Office Park
1700 West Park Drive
Westborough, Massachusetts 01581
Telephone: (508) 616-9660
Facsimile: (508) 616-9661

Attorney Docket No.: SUN03-06(P9621)

Dated: April 30, 2007